UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

| APPLICATION NO. | FILING DATE | FIRST NAMED INVENTOR | ATTORNEY DOCKET NO. | CONFIRMATION NO. |
|---|---|---|---|---|
| 09/651,548 | 08/29/2000 | Barry Atkins | RPS920000026US1 | 9903 |

42640 7590 06/28/2012

Yudell Isidore Ng Russell PLLC
8911 N. Capital of Texas Hwy.,
Suite 2110
Austin, TX 78759

| EXAMINER | |
|---|---|
| SHIN, KYUNG H | |

| ART UNIT | PAPER NUMBER |
|---|---|
| 2443 | |

| NOTIFICATION DATE | DELIVERY MODE |
|---|---|
| 06/28/2012 | ELECTRONIC |

**Please find below and/or attached an Office communication concerning this application or proceeding.**

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

Patents@yudellisidore.com

UNITED STATES PATENT AND TRADEMARK OFFICE

---

BEFORE THE BOARD OF PATENT APPEALS
AND INTERFERENCES

---

*Ex parte* BARRY ATKINS, DAVID CARROLL CHALLENER, FRANK NOVAK, JOSEPH GARY RUSNAK, KENNETH D. TIMMONS, and WILLIAM W. VETTER

---

Appeal 2010-002047
Application 09/651,548
Technology Center 2400

---

Before LANCE L. BARRY, MAHSHID D. SAADAT, and JEAN R. HOMERE, *Administrative Patent Judges*.

BARRY, *Administrative Patent Judge*.

DECISION ON APPEAL

STATEMENT OF THE CASE

The Patent Examiner rejected claims 1-24. The Appellants appeal therefrom under 35 U.S.C. § 134(a). We have jurisdiction under 35 U.S.C. § 6(b).

## INVENTION

The following claim illustrates the invention on appeal.

1. A method for managing a user key used to sign a message for a data processing system, said method comprising:

assigning a user key to a user and storing the user key in an encrypting data processing system utilized to encrypt messages;

encrypting the messages with the user key;

storing an associated key in the encrypting data processing system and encrypting the user key with the associated key to obtain an encrypted user key, wherein said associated key comprises a private key;

said encrypting data processing system communicating at least one encrypted message together with the encrypted user key to a recipient system in order to permit validation of an association of the user with the encrypted messages by the recipient system; and

thereafter, preventing validation of the association of the user with messages by revoking the associated key at the encrypting data processing system so that the encrypting data processing system is no longer able to decrypt the encrypted user key.

## REJECTIONS

Claims 1-4, 6-12, 14-20, and 22-24 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over U.S. Patent No. 6,807,277 B1 ("Doonan") and U.S. Patent No. 6,732,101 B1 ("Cook").

Claims 5, 13, and 21 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Doonan, Cook, and U.S. Patent No. 4,888,800 ("Marshall").

DISCUSSION

Based on the dependencies of the claims, we will decide the appeal of claims 1-24 on the basis of claims 1, 9, and 17.

The issues before us follows: Did the Examiner err in finding that Noonan teaches "encrypting [a] user key with [an] associated key to obtain an encrypted user key, wherein *said associated key comprises a private key*," as required by claim 1 and similarly required by claims 9 and 17? (Emphasis added.)

The question of obviousness is "based on underlying factual determinations including . . . what th[e] prior art teaches explicitly and inherently." *In re Zurko*, 258 F.3d 1379, 1383 (Fed. Cir. 2001) (citations omitted).

Here, the Examiner admits that "Doonan discloses that an . . . associated key is encrypted using a public key." (Ans. 10.) The Examiner makes the following findings.

> Doonan also discloses in different encryption procedures that a private key within a public/private key pair can be used to encrypt information such as a message or a key. (Doonan col 5, ll 63-67: generate an encrypted user key for transmission; col 5, ll 48-50: additionally; encrypted with a private key corresponding to digital certificate (private key used for information encryption; implies public key used for decryption) [.])

(Ans. 10.)

We agree with the Appellants that in column 5, lines 63-67, "*Doonan's* public key of the message recipient is relied upon . . . as disclosing the claimed 'associated key.' However, Claim[s] 1[, 9, and 17] explicitly recite[] that the 'associated key comprises a private key,' rather

than a public key as disclosed by *Doonan*." (App. Br. 11.) We further agree with the Appellants that in column 5, lines 48-50, "*Doonan[]* further discloses[es] . . . encrypting a hash of a message (rather than a user key as claimed)." (App. Br. 12.)

Furthermore, the Examiner does not allege, let alone show, that the addition of other applied references cures the aforementioned deficiency of Noonan.

Therefore, we conclude that the Examiner did err in finding that Noonan teaches "encrypting the user key with the associated key to obtain an encrypted user key, wherein *said associated key comprises a private key*," as required by claim 1 and similarly required by claims 9 and 17. (Emphasis added.)

## DECISION

We reverse the rejection of claim 1, 9, and 17 and those of claims 2-8, 10-16, and 18-24 which depend therefrom.

REVERSED

peb